## REMARKS

In view of the preceding amendments and the following remarks, the Applicant respectfully requests reconsideration of the present application.

## Rejection

The Office Action dated March 8, 2004, Paper No. 4 rejects claims 1-29 under 35 U.S.C. § 102(b) as being anticipated by United States Patent No. 5,804,703 entitled "Method and Apparatus for Digital Signature Authentication" which issued September 8, 1998, on an application filed by Richard E. Crandall ("the Crandall patent").

## The Cited Reference

The Crandall patent discloses:

> A **separate source 813**[1] stores publicly known information, such as the public keys "ourPub" and "theirPub" of sender 801 and receiver 802, the initial point ($x_1$, $y_1$), the field $F_{pk}$, and curve parameter "a". **This** [public] **source** [813] **of information** may be a published directory, an on-line source for use by computer systems, or **it**[, i.e. the public source 813,] **may transmitted between sender and receiver over a non-secure transmis-**

[1] Depicted both in FIG. 8 and in FIG. 12. "FIG. 8 is a block diagram of the present invention." (Col. 12, line 51.) "FIG. 12 illustrates a block diagram for implementing the digital signature scheme of the present invention." (Col. 19, lines 34-35.)

**sion medium**.[2] The public source 813 is shown symbolically connected to sender 801 through line 815 and to receiver 802 through line 814.[3] (Col. 13, lines 9-17.) (Emphasis supplied.)

The receiver 802 generates a deciphering key $D_K$ using the receiver's private key, theirPri. TheirPri is provided from the private key source 808 to the elliptic multiplier 804, along with sender's public key, ourPub, (from the **public source 813**). Deciphering key $D_K$ is generated from (theirPri)°(ourPub) (mod p). The deciphering key $D_K$ is equal to the enciphering key $e_K$ due to the abelian nature of the elliptic multiplication function. Therefore, the receiver 802 reverses the encryption scheme, using the deciphering key $D_K$, to recover the plaintext message Ptxt from the ciphertext message C. (Col. 13, lines 31-40.) (Emphasis supplied.)

The encryption/decryption means 1204 of receiver 1202 is coupled to elliptic multiplier 806 through line 810. The elliptic multiplier 806 is coupled to the private key source 808 through line 812. The point u is provided to the elliptic multiplier 806 from the nonsecure channel 816 via line 1212. Elliptic multiplier 806 generates point Q and provides it to comparator 1208 via line 1216. Hasher 1206 recieves (sic) the ciphertext message C and point P from nonsecure channel 816 via line 1210, and ourPub from **source 813** via line 1218. Hasher 1206 outputs point R to comparator 1208 via line 1214.

---

[2] How could the "public source 813" "of information," i.e. a physical location, be "transmitted between sender and receiver over a non-secure transmission medium" as described in the Crandall patent? What does this text truly mean? Does it perhaps mean that the sender 801 or 1201 and/or the receiver 802 or 1202 exchange pointers to locations of the "public source 813?"

[3] Note that lines 814 and 815, both in FIGs. 8 and 12, in all instances terminate in arrows that are directed away from rather than toward the public key source 813. Thus, FIGs. 8 and 12 teach away from storage of information or data either by the sender 801 or 1201 or by the receiver 802 or 1202 into the "public source 813."

(Col. 19, line 62 - col. 20, line 5.) (Emphasis supplied.)

A separate **source 813** stores publicly known information, such as the public keys "ourPub" and "theirPub" of sender 1201 and receiver 1202, the initial point ($x_1$, $y_1$), the field $F_{pk}$, and curve parameter "a". This source of information may be a published directory, an on-line source for use by computer systems, or it may transmitted between sender and receiver over a non-secure transmission medium.[4] The **public source 813** is shown symbolically connected to sender 1201 through line 815 and to receiver 1202 and hasher 1206 through lines 814 and 1218 respectively. (Col. 20, lines 15-24.) (Emphasis supplied.)

The receiver 1202 generates a deciphering key $D_K$ using the receiver's private key, theirPri. TheirPri is provided from the private key source 808 to the elliptic multiplier 806, along with sender's public key, ourPub, (from the **public source 813**). Deciphering key $D_K$ is generated from (theirPri)°(ourPub) (mod p). The deciphering key $D_K$ is equal to the enciphering key $e_K$ due to the abelian nature of the elliptic multiplication function. Therefore, the receiver 1202 reverses the encryption scheme, using the deciphering key $D_K$, to recover the plaintext message from the ciphertext message C.

The elliptic multiplier 806 of the receiver 1202 receives point u from the nonsecure channel 816. The elliptic multipler (sic) 806 generates point Q and provides it to comparator 1208. Hasher recieves (sic) the ciphertext message C and point P from the nonsecure channel 816 and the purported senders public key ourPub from **source 813** and generates point R, which it provides to comparator 1208. Comparator 1208 compares points Q and R and if they match, the signature is assumed to be

---

[4] As demonstrated by Exhibit A hereto, other than for the reference nos. 801, 1201 and 802, 1202 the text in column 20 of the Crandall patent at lines 15-21 is word-for-word identical to the text in column 13 at lines 9-15. Therefore, **footnotes 2 and 3 to the text in column 13 at lines 9-15 are equally applicable to the text in column 20 at lines 15-21**.

> valid. In the present invention, the comparison of points Q and R is accomplished using the optimized scheme using x values described above. (Col. 20, lines 42-63.) (Emphasis supplied.)

**The preceding excerpts** from the Crandall patent **present everything which that reference discloses about the "public source 813**." The Applicant respectfully submits that the Crandall patent fails to expressly disclose in its text, or implicitly disclose in its drawings, storage of any information or data into the "public source 813" either by a sender 801 or 1201 or by a receiver 802 or 1202.

Regarding the public data "**ourPub**" and "**theirPub**" stored in the "**source 813**" of publicly known information, in addition to the disclosures of "ourPub" and "theirPub" that appear above in the excerpts for the source 813, Exhibit 2 attached hereto presents **all** disclosures in the Crandall patent about "ourPub" and "theirPub." Applicant is unable to find anywhere in the excerpts from the Crandall patent set forth in Exhibit B any disclosure that a sender 801 or 1201 or a receiver 802 or 1202 stores anything into any source of publicly known information, particularly into the public source 813.

**Legal Principles Applicable to Rejections Under 35 U.S.C. 102(b)**

Certain well established principles are to be applied in assessing whether or not a reference anticipates a claim under 35 U.S.C. 102(b). First, the claims of a patent, which define the invention, are "to be construed in light of the specification and both are to be read with a view to ascertaining the invention." United States v. Adams, 383 U.S. 39, 49, 148 USPQ 479, 482 (1966). The "differences between the prior art and the claims at issue are to be ascertained." Graham v. John Deere Co., 383 U.S. 1, 17, 148 USPQ 459, 467 (1966). The prior art as a whole must be considered, and those portions of the prior art arguing against or teaching away from the claimed invention must be considered. Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc., 796 F.2d 443, 448, 230 USPQ 416, 420 (Fed. Cir. 1986), In re Hedges, et al., 783 F.2d 1038, 1041, 228 USPQ 685, 687 (Fed. Cir. 1986).

> [F]or anticipation under 35 U.S.C. § 102, the reference must teach **every aspect** of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. Manual of Patent Examining Procedure ("MPEP") Eighth Edition Revision 1, February 2003, § 706.02, p. 700-21 (Emphasis supplied)

"Anticipation under 35 U.S.C. § 102 requires the disclosure in a single piece of prior art of each and every limitation of a claimed invention." Rockwell International Corporation v. The United States, 147 F.3d 1358, 1363, 47 USPQ2d 1027, 1031 (Fed. Cir.

1998) citing National Presto Indus. v. West Bend Co., 76 F.3d 1184, 1189, 37 USPQ2d 1685, 1687 (Fed. Cir. 1966). In determining anticipation under 35 U.S.C. § 102, functional language, preambles, and language in "whereby," "thereby," and "adapted to" clauses cannot be disregarded. Pac-Tec, Inc. v. Amerce Corp., 903 F.2d 796, _____, 14 USPQ2d 1871, 1876 (Fed. Cir. 1990).

**Argument**

The preceding analysis of the cited reference establishes that the Crandall patent fails to disclose, either expressly or implicitly, storage of any information or data into any publicly accessible repository either by the sender 801 or 1201, or by the receiver 802 or 1202.

Pending independent claims 1, 10 and 19 all expressly require that a **receiving unit transmit a plurality of public quantities for storage in a publicly accessible repository**.

**Claim 1**

a. **the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities**

**Claim 10**

c. a pair of cryptographic units . . . , each cryptographic unit:
   i. **when the cryptographic unit is to receive the cyphertext message M:**
      (1) **storing plurality of public quantities in a publicly accessible repository**

**Claim 19**

A cryptographic unit . . . comprising:
a. ports:
   i. **when the cryptographic unit is to receive the cyphertext message M,** for:
      (1) **storing plurality of public quantities in a publicly accessible repository**

Pending independent claim 28 expressly requires that a **sending unit transmit a plurality of public quantities for storage in a publicly accessible repository**.

**Claim 28**

In a protocol for communication in which a sending unit S transmits onto the communication channel I a message "M" together with a digital signature, and, wherein before transmitting the message M and the digital signature, **the sending unit S transmits for storage in a publicly accessible repository a plurality of public quantities**, a method by which a receiving unit R that receives the message M and the digital signature verifies the authenticity of digital signature comprising the steps performed by the receiving unit R of:

Because **pending independent claims** 1, 10, 19 and 28 all **expressly require storage of a plurality of public quantities in a publicly accessible repository**, and because the Crandall patent fails to disclose, either expressly or implicitly, storage of any

information or data into the "public source 813" either by the sender 801 or 1201 or by the receiver 802 or 1202, based upon the controlling legal authority cited above the Applicant respectfully submits that:

1. independent claims 1, 10, 19 and 28 now pending in this patent application all traverse rejection under 35 U.S.C. § 102(b) as being anticipated by the Crandall patent, and are therefore allowable;
2. dependent claims 2-9, 11-18, 20-27 and 29 now pending in this patent application, because they depend respectively from one of the allowable independent claims 1, 10, 19 and 28, also all traverse rejection under 35 U.S.C. § 102(b) as being anticipated by the Crandall patent, and are therefore allowable; and
3. therefore, claims 1-29 now pending in this patent application are all allowable.

Furthermore, Applicant observes that for the following reason even if, contrary to fact, the Crandall patent were to disclose, either expressly or implicitly, storage of any information or data into the "public source 813" either by a sender 801 or 1201 or by a receiver 802 or 1202, that reference could not anticipate any of the claims now pending in this patent application. The Crandall patent discloses that the "public source 813" stores only two

quantities, i.e. "ourPub" and "theirPub." The Crandall patent further discloses that **the sender 801 or 1201 and the receiver 802 or 1202 each respectively have only one public key**:

1. **ourPub**; and
2. **theirPub**. (For example, col. 15 at lines 34-38.)[5]

Consequently, even if the Crandall patent were to disclose, either expressly or implicitly, storage of any information or data into the "public source 813," **that reference could not possibly disclose storage of a plurality of public quantities in a publicly accessible repository** either:

1. by the sender 801 or 1201; or
2. by the receiver 802 or 1202.

Since the sender 801 or 1201 and the receiver 802 or 1202 each have only one public quantity, i.e. respectively **ourPub** and **theirPub**, **at best they could respectively store only that one quantity into the "public source 813**." As demonstratede above, independent claims 1,

---

[5] Security and authentication considerations compel generation of the public keys **ourPub** and **theirPub** respectively:
1. independently by the sender 801 or 1201 and by the receiver 802 or 1202; or
2. by a neutral, trusted third party.

If either only the sender 801 or 1201 or only the receiver 802 or 1202 were to generate both the public keys **ourPub** and **theirPub**, then the sender 801 or 1201 or the receiver 802 or 1202 which generated both the public keys **ourPub** and **theirPub** could create bogus communications allegedly sent by whichever unit did not generate its respective public key **ourPub** or **theirPub**.

10, 19 and 28 now pending in this patent application all expressly require **storage of a plurality of public quantities in a publicly accessible repository** either:

1. by the receiver, independent claims 1, 10 and 19; or
2. by the sender, independent claim 28.

**Conclusion**

Since for the preceding reasons the Crandall patent:

1. fails to disclose, either expressly or implicitly, storage of any information or data into the "public source 813" either by a sender 801 or 1201 or by a receiver 802 or 1202; and
2. even if the reference were to disclose, either expressly or implicitly, storage of any information or data into the "public source 813," the reference could not disclose storage of a plurality of public quantities into a publicly accessible repository;

the reference can not anticipate under 35 U.S.C. § 102(b) independent claims 1, 10, 19 or 28. Because for both of the preceding reasons the Crandall patent does not anticipate independent claims 1, 10, 19 or 28, the Applicant respectfully:

1. submits that pending claims 1-29 are allowable over the Crandall patent; and

2. requests that this patent application pass promptly to issue.

Respectfully submitted

Donald E. Schreiber
Reg. No. 29,435

Dated: 8 July, 2004

Donald E. Schreiber
A Professional Corporation
Post Office Box 2926
Kings Beach, CA 96143-2926

Telephone: (530) 546-6041

Attorney for Applicant

Exhibit A

**A Comparison of Differences Between the Crandall Patent's Texts Excerpted Respectively from Column 13 at Lines 9-15 and Column 20 at Lines 15-21**

A separate source 813 stores publicly known information, such as the public keys "ourPub" and "theirPub" of sender ~~801~~ 1201 and receiver ~~802~~ 1202, the initial point $(x_1, y_1)$, the field $F_{pk}$, and curve parameter "a". This source of information may be a published directory, an on-line source for use by computer systems, or it may transmitted between sender and receiver over a non-secure transmission medium.

Exhibit B

**The Crandall Patent's Disclosures Concerning "ourPub" and "theirPub"**

In a Diffie-Hellman system, a directory of public keys is published or otherwise made available to the public. A given public key is dependent on its associated private key, known only to a user. However, it is not feasible to determine the private key from the public key. For example, a sender has a public key, referred to as "**ourPub**". A receiver has a public key, referred to here as "**theirPub**". The sender also has a private key, referred to here as "myPri". Similarly, the receiver has a private key, referred to here as "theirPri".

There are a number of elements that are publicly known in a public key system. In the case of the Diffie-Hellman system, these elements include a prime number p and a primitive element g. p and g are both publicly known. Public keys are then generated by raising g to the private key power (mod p). For example, a sender's public key **myPub** is generated by the following equation:

$$\mathbf{myPub} = g^{myPri} \pmod{p} \qquad \text{Equation (1)}$$

Similarly, the receiver's public key is generated by the equation:

$$\mathbf{theirPub} = g^{theirPri} \pmod{p} \qquad \text{Equation (2)}$$

(Col. 3, lines 6-29.)

FIG. 2 illustrates a flow chart that is an example of a key exchange using a Diffie-Hellman type system. At step 201, a prime number p is chosen. This prime number p is public. Next, at step 202, a primitive root g is chosen. This number g is also publicly known. At step 203 an enciphering key $e_K$ is generated, the receiver's public key (**theirPub**) is raised to the power of the sender's private key (myPri). That is:

$$(\mathbf{theirPub})^{myPri} \pmod{p} \qquad \text{Equation (3)}$$

We have already defined **theirPub** equal to $g^{theirPri} \pmod{p}$. Therefore Equation 3 can be given by:

$$(g^{theirPri})^{myPri} \pmod{p} \qquad \text{Equation (4)}$$

(Col. 3, lines 38-66.)

This value is the enciphering key $e_K$ that is used to encipher the plaintext message and create a ciphertext message. The

particular method for enciphering or encrypting the message may be any one of several well known methods. Whichever encrypting message is used, the cipher key is the value calculated in Equation 4. The ciphertext message is then sent to the receiver at step 204.

At step 205, the receiver generates a deciphering key $D_K$ by raising the public key of the sender (myPri)[1] to the private key of the receiver (theirPri) as follows:

$$D_K = (\mathbf{myPub})^{theirPri} \pmod{p} \qquad \text{Equation (5)}$$

From Equation 1, **myPub** is equal to $g^{myPri} \pmod{p}$. (Col. 3, lines 6-29.)

AUTHENTICATION

* * *

Another scheme of digital signature authentication is a generalization of the ElGamal discrete logarithm scheme, using elliptic algebra. Assume a public key **ourPub** generated with a function of a private key ourPri. The signature is generated by first choosing a random integer m of approximately q bits. Next a point $P = m°(X_1/1)$ is computed. A message digest function M is used to compute an integer u that is a function of m, ourPri, and the digested version of the ciphertext message and the computed point P. The computed pair (u, P) is transmitted as the signature.

At the receiving end, the u value of the signature is used to compute the point $Q = u°(X1/1)$. A point R is calculated using P, the digested version of the ciphertext message and P, and **myPub**. If R and Q do not compare exactly, the signature is not valid (not genuine). The security of this scheme relies on the computational infeasability of breaking the elliptic logarithm operation or the hash function M. A disadvantage of this scheme is that it is computationally intensive, making it complex and slow in operation. (Col. 4, line 37 - col. 5, line 7.)

---

[1] While the text "(miPri)" appears in the Crandall patent, it appears from the immediately preceding words and from Equation 5 that the text is erroneous and should instead be "(myPub)."

Elliptic Curve Public Key Exchange

It is necessary that both sender and recipient use the same set of such parameters. Both sender and recipient generate a mutual one-time pad, as a particular x-coordinate on the elliptic curve.

In the following description, the terms "our" and "our end" refer to the sender. The terms "their" and "their end" refer to the receiver. This convention is used because the key exchange of the present invention may be accomplished between one or more senders and one or more receivers. Thus, "our" and "our end" and "their" and "their end" refers to one or more senders and receivers, respectively.

The public key exchange of the elliptic curve cryptosystem of the present invention is illustrated in the flow diagram of FIG. 3.

Step 301--At our end, a public key is computed: **ourPub** $\epsilon$ $F_{pk}$

$$\textbf{ourPub} = (\text{ourPri}) \circ (x_1, y_1) \qquad \text{Equation (12)}$$

Step 302--At their end, a public key is computed: **theirPub** $\epsilon$ $F_{pk}$

$$\textbf{theirPub} = (\text{theirPri}) \circ (x_1, y_1) \qquad \text{Equation (13)}$$

Step 303--The two public keys **ourPub** and **theirpub**[2] are published, and therefore known to all users.

Step 304--A one-time pad is computed at our end: ourPad $\epsilon$ $F_{pk}$

$$\text{ourPad} = (\text{ourPri}) \circ (\textbf{theirpub}^3) = (\text{ourPri}) \circ (\text{theirPri}) \circ (x_1, y_1) \qquad \text{Equation (14)}$$

Step 305--A one-time pad is computed at their end: theirPad $\epsilon$ $F_{pk}$

$$\text{theirPad} = (\text{theirPri}) \circ (\textbf{ourPub}) = (\text{theirPri}) \circ (\text{ourPri}) \circ (x_1, y_1) \qquad \text{Equation (15)}$$

(Col. 7, line 63 - col. 8, line 33.)

---

[2] It appears that capitalization has been omitted from this text, and it should properly be "theirPub."

[3] It appears that capitalization has been omitted from this text, and it should properly be "theirPub."

In operation, the sender and receiver generate a common one time pad for use as an enciphering and deciphering key in a secure transmission. The private key of the sender, ourPri, is provided to the elliptic multiplier 805, along with the sender's public key, **theirPub**. The elliptic multiplier 805 computes an enciphering key $e_K$ from (ourPri)°(**theirPub**) (mod p). The enciphering key is provided to the encryption/decryption means 803, along with the plaintext message Ptxt. The enciphering key is used with an encrypting scheme, such as the DES scheme or the elliptic curve scheme of the present invention, to generate a ciphertext message C. The ciphertext message is transmitted to the receiver 802 over a nonsecure channel 816. (Col. 13, lines 18-30.)

Using both fast class numbers and inversionless parameterization, a public key exchange using the method of the present invention can proceed as follows. In the following example, the prime is a Mersenne prime. However, any of the fast class numbers described herein may be substituted.

1) At "our" end, use parameter a, to compute a public key: **ourPub** $\epsilon$ $F_{pk}$
(X/Z) = ourPri°$(X_1/1)$
**ourPub** = $XZ^{-1}$
2) At "their" end, use parameter a, to compute a public key: **theirPub** $\epsilon$ $F_{pk}$
(X/Z) = theirPri°$(X_1/1)$
**theirPub** = $XZ^{-1}$
3) The two public keys **ourPub** and **theirPub** are published, and therefore are known.
4) Compute a one-time pad: ourPad $\epsilon$ $F_{pk}$
(X/Z) = ourPri°(**theirPub**/1)
ourPad = $XZ^{-1}$
5) Compute a one-time pad: theirPad $\epsilon$ $F_{pk}$
(X/Z) = theirPri°(**ourPub**/1)
theirPad = $XZ^{-1}$
The usual key exchange has been completed, with
ourPad = theirPad
Message encryption/decryption between "our" end and "their" end may proceed according to this mutual pad. (Col. 14, lines 28-54.)

At step 905, the sender computes $X_1/Z$ = ourPri°$(X_1/1)$ using inversionless parameterization. The sender's public key is gener-

ated **ourPub** = $(XZ^{-1})(\text{mod } p)$. The receiver's public key **theirPub** = $(XZ^{-1})(\text{mod } p)$, is generated at step 906.

A one time pad for the sender, ourpad, is generated at step 907. X/Z = ourPri)[4]°(**theirPub**/1). ourPad = $XZ^{-1}(\text{mod } p)$. At step 908, a one time pad for he receiver, theirPad, is generated. X/Z = (theirPri)°(**ourPub**/1). theirPad = $XZ^{-1}(\text{mod } p)$. The calculation of ourPad and theirPad utilizes FFT multiplies to eliminate the need to calculate the inversion $Z^{-1}$. At step 909, the sender converts a plaintext message Ptxt to a ciphertext message C using ourPad. The ciphertext message C is transmitted to the receiver. At step 910, the receiver recovers the plaintext message Ptxt by deciphering the ciphertext message C using theirPad. (Col. 15, lines 34-49.)

Creation of Signature

Assume a curve parameterized by a, with starting point $(X_1/1)$. The sender's public key **ourPub** is generated as the multiple ourPri°$(x_1/1)$, where ourPri is our private key (an integer) and ° is multiplication on the elliptic curve. The digital signature is created as follows:

1) Choose a random integer m of approximately q bits.
2) Compute the point

$$P = m°(X_1/1).$$

3) Using a message digest function M, compute the integer

$$u = m + \text{ourPri}*M(\text{ciphertext}, P)$$

where ciphertext is the encrypted message to be sent.

4) Along with the ciphertext, transmit the digital signature as the pair (u, P). Note that u is an integer of about $2^q$ bits, while P is a point on the curve. (Col. 16, lines 37-56.)

Authentication of Digital Signature

The receiver attempts to authenticate the signature by generating a pair of points to match the digital signature pair, using the ciphertext message and the public key of the puported

---

[4] It appears that the text of the Crandall patent omits a "(," and that the text should properly be "(ourPri)."

sender. The receiver verifies the signature using the following steps:

1) Using the u part of the signature, compute the point

$$Q = u \circ (X_1/1)$$

2) Compare the point Q to the point

$$R = P + M(\text{ciphertext}, P) \circ \textbf{ourPub}$$

The signature is invalid if these elliptic points Q and R do not compare exactly. In other words, if the signature is authentic, the following must hold:

$$u \circ (X_1/1) = P + M(\text{ciphertext}, P) \circ \textbf{ourPub}$$

Substituting for u on the left side of the equation above gives:

$$(m + \text{ourPri} * M(\text{ciphertext}, P)) \circ (X_1/1) = P + M(\text{ciphertext}, P) \circ \textbf{ourPub}$$

or:

$$m \circ (X_1/1) + (\text{ourPri} * M(\text{ciphertext}, P)) \circ (X_1/1) = P + M(\text{ciphertext}, P) \circ \textbf{ourPub}$$

Substituting for **ourPub** on the right side of the equation yields:

$$m \circ (X_1/1) + (\text{ourPri} * M(\text{ciphertext}, P)) \circ (X_1/1) = P + M(\text{ciphertext}, P) \circ \text{ourPri} \circ (X_1/1)$$

(Col. 16, line 62 - col. 17, line 34.)

Security

The digital signature scheme of this scheme is secure on the basis of the following observation. To forge a signature one would need to find a pair (u, P) and a ciphertext that satisfy the equation

$$u \circ (X_1/1) = P + M(\text{ciphertext}, P) \circ \textbf{ourPub}$$

This would either entail an elliptic logarithm operation (the basis of the encryption security of the present invention) or breaking of the hash function M.

Optimizing Authentication

The recipient's final step in the digital signature scheme of the present invention involves the addition of two points; namely P and M(ciphertext, P)°**ourPub** to yield R and comparing that sum to a point Q. One could perform the elliptic addition using specified y-coordinates at each step. The scheme of the present invention provides a method of deducing the possible values of the x-coordinate of a sum of two points, using only the respective x-coordinates of the original two points in question. Using this method one may rapidly perform a necessity check on whether the points Q and the sum of P+M(ciphertext, P)°**ourPub** have identical x-coordinates. (Col. 17, line 51 - col. 18, line 8.)

In practical application, $P_1$ represents the calculated point P that is sent as part of the signature by the sender. $P_2$ represents the expression M(ciphertext, P)°**ourPub**. Q of course represents $u°(X_1/1)$. $P_1 + P_2$ represents R and is compared to Q. (Col. 18, lines 50-54.)

At step 1103 a point P2 is generated using **ourPub** and the ciphertext message. In the preferred embodiment, the relationship M(ciphertext, P)°**ourPub** is used to generate P2. Other relationships may be used depending on what relationships were used to calculate u, P by the sender. (Col. 19, lines 17-21.)

A function to calculate Q and compare it with (P+M(ciphertext, P)°**ourPub**) is as follows:

```
q = new_public_from_private (NULL, depth, seed);
elliptic_mul (q, u); /* u is the random integer. */
elliptic_mul (our, m); /* m = M(cipertext, P). */
/* Next, use the transmitted point p. */
if(signature_compare (p, our, q))
     fprintf(stderr,"Signature invalid.\n");
```